**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|---|---|
| In re Application of: | : | Conf. #4126 |
| Michael G. Lee, et al. | : | Group Art Unit: 2134 |
| Appln. No.: 09/865,667 | : | |
| | : | Examiner: Andrew L. Nalven |
| Filed: May 29, 2001 | : | |

For: METHOD AND APPARATUS FOR SECURELY TRANSMITTING ENCRYPTED DATA THROUGH A FIREWALL AND FOR MONITORING USER TRAFFIC

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**PRE-APPEAL BRIEF REQUEST FOR REVIEW**

Pursuant to the Pre-Appeal Brief Conference Pilot Program announced in the Official Gazette, Applicant hereby requests a pre-appeal brief conference in the above-referenced patent application. No amendments are being filed with this request. Additionally, this request is being filed with a Notice of Appeal. The review is requested for the reasons stated below.

The present application was filed on May 29, 2001. On September 9, 2004, an initial action was issued rejecting claims 1-2, 4-8, and 10-12 under 35 U.S.C. § 102(e) as being anticipated by Perlman (U.S. Patent No. 6,546,486) and claims 3 and 9 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Perlman in view of Ylonen (U.S. Patent No. 6,438,612, hereinafter "Ylonen"). Despite various attempts to distinguish the present patent application from the cited references, the Office has maintained its rejections of claims 1-12, which are certain to be overturned on appeal. Rather than further time being spent addressing these references, Applicants have elected to pursue the new pilot program.

As set forth in greater detail in Applicant's responses dated December 21, 2004, May 18, 2005, June 30, 2005, November 28, 2005, and April 28, 2006, the cited references, taken either

alone or in combination, fail to disclose, or even suggest, the elements set forth in the pending claims.

**REJECTIONS UNDER 35 U.S.C. § 102(e)**

Claims 1-2, 4-8, and 10-12 were rejected under 35 U.S.C. § 102(e) as being anticipated by Perlman (U.S. Patent No. 6,546,486). Specifically, regarding claim 1, Applicant respectfully submit that Pearlman fails to teach or suggest "a method for enabling a firewall to securely pass encrypted data, the method comprising detecting an exchange of a first encryption key between a host device and a remote device…exchanging a second encryptions key…requesting at the firewall…and passing encrypted data when it is determined that the first encryption key is received" as expressly recited in claim 1.

The Examiner asserts that the claimed "second key" is disclosed by the firewall public key of Perlman. *See* Office Action filed February 28, 2006 at p. 2. Applicants respectfully submit that if the claimed "second key" is the firewall public key, then Perlman fails to disclose the claimed "detection of an exchange of a first encryption key between a host device and a remote device."

The Examiner relies on col. 4, lines 63-66, to allegedly disclose this feature. The cited portion refers to "message key 204" for use in encrypting a message between source 102 and destination 110. However, as disclosed in Perlman (and relied upon by the Examiner) it is message key 306 that is detected. Col. 5, lines 55-67. Key 204 (i.e., the alleged claimed "first key") is not detected, but rather is passed to destination 110 for decryption at the destination. *Id.* Therefore, even if Perlman's "public key" is considered to be the claimed "second key," then Perlman fails to disclose the claimed features of the "first key."

In the Advisory Action filed on June 7, 2006, the Examiner asserts that key 204 is "detected as it passes through the firewall and when it receives the security association (Perlman, column 5 lines 1-6)" by relying on the assertion that "message key 306 is detected by the firewall as it is exchanged between source and destination through the firewall (Perlman, column 5 lines 54-56)." The Examiner acknowledges that Perlman does not teach that key 204 is detect. Rather, the basis for the Examiner's assertion appears to be that since key 204 is "merely

one embodiment of the invention" and key 306 is presumably detected in a "second embodiment", the keys are, in effect, interchangeable with each other. However, Applicant respectfully disagrees.

Applicant respectfully submits that the Examiner's picking and choosing components from differing embodiments of Perlman is improper. For example, key 204 of Perlman is directed to an embodiment where content screening is within a firewall that encrypts a message 202 with a message key 204 for "a single packet, or alternatively a group of packets that collectively form a single message." *See* Perlman at col. 4, lines 56-62; fig. 2. On the other hand, key 306 is directed to a different embodiment where the message is a "self-contained message". *See* Perlman at col. 5, lines 38-54; Fig. 3. Furthermore, even assuming that Examiner's picking and choosing components from different embodiments of Perlman is proper, Applicant respectfully submits that there is no disclosure, teaching, or suggestion to permit such an interchangeability of parts. In fact, Perlman discloses separate embodiments to describe to emphasize different features and functionalities of content screening "in more detail" based on separate and distinct embodiments. As discussed above, the keys of Perlman serve different purposes. Key 204 is not detected, but rather is passed to destination 110 for decryption at the destination. Thus, if Perlman's "public key" is considered to be the claimed "second key," then Perlman fails to disclose the claimed features of the "first key." As a result, the allegedly detection of key 306 does not suffice to teach or suggest that key 204 is detected.

Accordingly, for at least these reasons, Applicants respectfully submit that the rejections of claims 1, 4, 5, 7 and 10-11 are improper and request that they be withdrawn.

Claims 2, 6, 8 and 12 depend from one of claims 1, 7 or 11 and, thus, contain the features recited therein. As discussed above, Perlman fails to disclose or suggest each feature recited in the independent claims. For at least these reasons, Applicants respectfully submit that the rejections of claims 2, 6, 8 and 12 are also improper and respectfully request that they be withdrawn.

**REJECTIONS UNDER 35 U.S.C. § 103**

Claims 3 and 9 were rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Perlman in view of Ylonen. Claims 3 and 9 depend from claims 1 and 7 respectively and, as such, contain the features recited in the independent claims. Ylonen is relied upon to disclose the use of IKE protocols and, as such, fails to repair the above detailed deficiencies of Perlman. Nowhere in Ylonen is there a disclosure, teaching, or suggestion of "detecting an exchange of a first encryption key…exchanging a second encryption key…", as recited in the independent claims 1 and 7. For at least these reasons, Applicants respectfully submit that the rejections of claims 3 and 9 are improper and request that they be withdrawn.

**CONCLUSION**

In view of the foregoing, it is respectfully submitted that the rejections of claims 1-12 is in error. Accordingly, for the foregoing reasons, Applicant requests an appeal conference be convened so as to advise Applicant whether the Office will: 1) allow the present claims; 2) reopen prosecution and issue a new office action; or 3) allow this case to proceed to appeal.

Please charge any shortage in fees due in connection with the filing of this communication to Deposit Account No. 50-0206, and please credit any excess fees to such deposit account.

Respectfully submitted,

Hunton & Williams LLP

By: _____
George Y. Wang
Registration No. 58,637
For Christopher J. Cuneo
Registration No. 42,450

Hunton & Williams LLP
1900 K Street, N.W.
Washington, D.C. 20006-1109
Telephone: (202) 955-1500
Facsimile: (202) 778-2201

Date: June 28, 2006